UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/767,284	01/22/2001	Eliot Lear	50325-0517	2045

7590   06/14/2005

Hickman Palermo Truong & Becker, LLP
1600 Willow Street
San Jose, CA 95125-5106

EXAMINER
KLIMACH, PAULA W

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 06/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/767,284	LEAR ET AL.
	Examiner	Art Unit	
	Paula W. Klimach	2135	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 March 2005*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6 and 13-24* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6 and 13-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date *03/28*.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 03/28/05. Applicant cancelled

Claims 7-12, and amended Claims 1, 13, 19, 20, and 23-24. The amendment filed on 03/28/05

have been entered and made of record. Therefore, presently pending claims are 1-6 and 13-24.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

Claims 1-6, 13-20 and 23-24 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Reid et al (6,182,226 B1) in view of Ray et al (6,587,455 B1) and further in view of Cheng

et al. (6,823,462 B1).

In reference to claim 1, Reid discloses a method of selectively enforcing a security policy

in a network, the method comprising the computer-implemented steps of creating and storing one

or more access controls in a policy enforcement point device that controls access of clients to the

network, wherein each of the access controls specifies that a named abstract group is allowed

access to a particular resource (column 4 line 49 to column 5 line 25). The regions defined by

Reid are created and stored in the firewall where it applies rules to the incoming packets (column

3 line 65 to column 4 line 10); therefore controlling access on opposite sides of the gateway.

The packets on opposite sides of the firewall are permitted to pass from the policy enforcement

point (firewall) into the network only if the network address is in the named group identified in

one of the access controls that specifies that the named group is allowed access to the network

(column 6 lines 21-31).

The applicant does not define binding a network address to an authenticated user. The

definition of binding is: imposing an obligation. Therefore binding a network address to an

authenticated user is imposing an obligation on that authenticated user. Although Reid discloses

a system wherein the device is authenticated in a virtual network (column 8 lines 40-59), Reid

does not disclose receiving, from an external binding process, a binding of a network address;

updating the named group to include the bound network address, and thus imposing an

obligation on that authenticated user.

Ray discloses a method for allocation of a network address associated with a virtual

subnet. The address server disclosed by Ray sends the network device an assigned network

address, assigned by the address server and therefore assigned from an external binding process

(column4 line 65 to column 5 line 31). The firewall saves the network address (column 6 line 66

to column 7 line 6) and therefore updates the group to include the new IP address.

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to automatically add nodes to the group as disclosed by Ray in the system of Reid.

One of ordinary skill in the art would have been motivated to do this because when a network

device initially connects to a network the device seeks an address server from which to request a

network address, when done by the network administrator, it is a time consuming task,

performing the task automatically saves time.

Although Ray discloses assigning the address by the address server, Ray does not disclose the server receiving the address from and information defining one more group lists, resource definitions, and definitions of users as members of one or more groups in the group lists, wherein the definitions include network addresses for the users, wherein the network addresses have been assigned by an address server.

Cheng discloses a system that receives information defining one or more group lists, resource definitions, and definitions of users as members of one or more groups in the group lists, wherein the definitions include network addresses for the user (column 7 lines 5-15 in combination with lines 16-19).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to receive information defining one or more group lists as in Cheng in the system of Ray. One of ordinary skill in the art would have been motivated to do this because it would alleviate the task of managing the security policy (Cheng column 1 lines 56-63).

In reference to claims 13, 19, and 20, Reid discloses a method of selectively enforcing a security policy in a network, the method comprising the computer-implemented steps of creating and storing one or more access controls in a policy enforcement point device that controls access of clients to the network, wherein each of the access controls specifies that a named abstract group is allowed access to a particular resource (column 4 line 49 to column 5 line 25). The regions defined by Reid are created and stored in the firewall where it applies rules to the incoming packets (column 3 line 65 to column 4 line 10); therefore controlling access on opposite sides of the gateway. The packets on opposite sides of the firewall are permitted to pass from the policy enforcement point (firewall) into the network only if the network address is in

the named group identified in one of the access controls that specifies that the named group is

allowed access to the network (column 6 lines 21-31). The user in the system disclosed by Reid

is an authenticated device (column 8 lines 40-59).

The applicant does not define binding a network address to an authenticated user. The

definition of binding is: imposing an obligation. Therefore binding a network address to an

authenticated user is imposing an obligation on that authenticated user. Although Reid discloses

a system wherein the device is authenticated in a virtual network (column 8 lines 40-59), Reid

does not disclose receiving, from an external binding process, a binding of a network address;

updating the named group to include the bound network address, and thus imposing an

obligation on that authenticated user.

Ray discloses a method for allocation of a network address associated with a virtual

subnet. The address server disclosed by Ray sends the network device an assigned network

address, receives the address of the new network device (column4 line 65 to column 5 line 31).

The firewall saves the network address (column 6 line 66 to column 7 line 6) and therefore

updates the group to include the new IP address.

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to automatically add nodes to the group as disclosed by Ray in the system of Reid.

One of ordinary skill in the art would have been motivated to do this because when a network

device initially connects to a network the device seeks an address server from which to request a

network address, when done by the network administrator, it is a time consuming task,

performing the task automatically saves time.

In reference to claim 24, Reid discloses a method of selectively enforcing a security

policy in a network, the method comprising the computer-implemented steps of creating and

storing one or more access control list entries in a network router that acts as a policy

enforcement point device and that controls access of clients to the network, wherein each of the

access control list entries specifies that a named group of users is allowed or refused access to a

particular network resource (column 4 line 49 to column 5 line 25). Reid also creates and stores

one or more definitions of the named groups in a data store that is accessible by the network

router (column 3 line 65 to column 4 line 10). The method disclosed by Reid protects the flow

of traffic from every region to every other region (column 5 lines 34-50) thereby permitting a

packet flow originating from the bound network address to pass from the policy enforcement

point into the network only if the bound network address is in the named group identified in one

of the access control list entries that specifies that the named group is allowed access to the

network. Regarding determining that the user has discontinued use of the client, and deleting the

network address to which the user is bound from each named group of each policy enforcement

point of the network (Reid column 15 lines 29-49). Reid discloses a function that is used to

modify and delete regions, this would include when a user has discontinued use of the client.

The applicant does not define binding a network address to an authenticated user. The

definition of binding is: imposing an obligation. Therefore binding a network address to an

authenticated user is imposing an obligation on that authenticated user. Although Reid discloses

a system wherein the device is authenticated in a virtual network (column 8 lines 40-59), Reid

does not disclose receiving, from an external binding process, a binding of a network address;

updating the named group to include the bound network address, and thus imposing an

obligation on that authenticated user.

　Ray discloses a method for allocation of a network address associated with a virtual

subnet. The address server disclosed by Ray sends the network device an assigned network

address, assigned by the address server and therefore assigned from an external binding process

(column4 line 65 to column 5 line 31). The firewall saves the network address (column 6 line 66

to column 7 line 6) and therefore updates the group to include the new IP address. Ray discloses

a system in which the network address is distributed to other nodes including policy enforcement

points (firewalls/gateway server) (column 6 lines 4-10 in combination with line 66 to column 7

line 6). The address server also sends the address of the network device to the device in the

subnet (group); the address is information identifying the group that the network device belongs

to because it is only sent to the devices in the subnet.

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to automatically add nodes to the group as disclosed by Ray in the system of Reid.

One of ordinary skill in the art would have been motivated to do this because when a network

device initially connects to a network the device seeks an address server from which to request a

network address, when done by the network administrator, it is a time consuming task,

performing the task automatically saves time.

In reference to claims 2 and 14, wherein the access control point (firewall) contains

definitions of groups and resources (service) as shown below. Definitions of groups are created

and stored in the firewall (column 5 lines 14-25). Definitions of resources (services) are stored

in the firewall/gateway (column 5 lines 33-49). Creating and storing one or more access controls

at the policy enforcement point, wherein each of the access controls specifies that a named group

is allowed access to a particular resource (service) (column 5 lines 8-25 in combination with

lines 34-49). Reid indicates that the groups (regions) are named (column 5 lines 14-24) and

stored in the firewall, since Reid discloses the access definition is stored in the firewall (column

5 lines 33-36). One of the access controls specifies that all other traffic is denied access to the

network (column 5 lines 37-38). The regions can only communicate with each other if there

exists an appropriate access rule. The system does not allow traffic to pass directly through

(column 5 lines 44-46); therefore all other traffic is denied access to the network.

In reference to claims 3 and 15, Reid does not disclose the steps of distributing the

network address of the user and information identifying one or more groups of which the

authenticated user is a member to all policy enforcement points of a protected network that the

user seeks to access.

Ray discloses a system in which the network address is distributed to other nodes

including policy enforcement points (firewalls/gateway server) (column 6 lines 4-10 in

combination with line 66 to column 7 line 6). The address server also sends the address of the

network device to the device in the subnet (group); the address is information identifying the

group that the network device belongs to because it is only sent to the devices in the subnet.

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to distribute the address of the user and the information identifying the group of

which the authenticated user is a member as shown in the system disclosed by Ray in the system

of Reid. One of ordinary skill in the art would have been motivated to do this because firewall

controls the information that passes between the external and internal network and therefore requires knowledge of which devices are in the networks.

In reference to claims 4 and 16, although Reid discloses the policy enforcement points (firewall) that define a security zone that encompasses the user (Figure 1; Secure Zone), Reid does not disclose the steps of distributing the network address of the user and information identifying one or more groups of which the authenticated user is a member to all policy enforcement points of a protected network that the user seeks to access.

Ray discloses a system in which the network address is distributed to other nodes including policy enforcement points (firewalls/gateway server) (column 6 lines 4-10 in combination with line 66 to column 7 line 6). The address server also sends the address of the network device to the device in the subnet (group); the address is information identifying the group that the network device belongs to because it is only sent to the devices in the subnet.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to distribute the address of the user and the information identifying the group of which the authenticated user is a member as shown in the system disclosed by Ray in the system of Reid. One of ordinary skill in the art would have been motivated to do this because firewall controls the information that passes between the external and internal network and therefore requires knowledge of which devices are in the networks.

In reference to claim 5, Reid does not disclose the policy enforcement point receiving an Internet Protocol (IP) address for the user from a network address binding resolution (NABR) process.

Ray discloses the firewall (policy enforcement point) receiving the IP address from the

network device (NABR process; column 6 line 66 to column 7 line 7).

At the time the invention was made, it would have been obvious to a person of ordinary skill in

the art to distribute the address of the user and the information identifying the group of which the

authenticated user is a member as shown in the system disclosed by Ray in the system of Reid.

One of ordinary skill in the art would have been motivated to do this because firewall controls

the information that passes between the external and internal network and therefore requires

knowledge of which devices are in the networks.

In reference to claims 6 and 18, further comprising the steps of determining that the user

has discontinued use of the client, and deleting the network address to which the user is bound

from each named group of each policy enforcement point of the network (Reid column 15 lines

29-49). Reid discloses a function that is used to modify and delete regions, this would include

when a user has discontinued use of the client.

In reference to claim 23, Reid discloses a method of selectively enforcing a security

policy in a network, the method comprising the computer-implemented steps of creating and

storing one or more access control list entries in a network router that acts as a policy

enforcement point device and that controls access of clients to the network, wherein each of the

access control list entries specifies that a named group of users is allowed or refused access to a

particular network resource (column 4 line 49 to column 5 line 25). Reid teaches that the

firewall is the policy enforcement point (system which enforces a security policy) and is

developed on the model of a screening router (column 1 lines 22-26). Therefore the router in the

system disclosed by Reid acts as a policy enforcement point. Reid also teaches creating and

storing one or more definitions of the named groups in a data store that is accessible by the

network router (column 6 lines 21-31). The user in the system disclosed by Reid is an

authenticated device (column 8 lines 40-59). The method disclosed by Reid protects the flow of

traffic from every region to every other region (column 5 lines 34-50) thereby permitting a

packet flow originating from the bound network address to pass from the policy enforcement

point into the network only if the bound network address is in the named group identified in one

of the access control list entries that specifies that the named group is allowed access to the

network.

Reid does not disclose receiving from an external process that can bind a user to a

specific network address, a binding of a network address and updating the named group to

include the bound network address

Ray discloses a method for allocation of a network address associated with a virtual

subnet. The address server disclosed by Ray sends the network device an assigned network

address, assigned by the address server and therefore assigned from an external binding process

(column4 line 65 to column 5 line 31). The firewall saves the network address (column 6 line 66

to column 7 line 6) and therefore updates the group to included the new IP address.

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to automatically add nodes to the group as disclosed by Ray in the system of Reid.

One of ordinary skill in the art would have been motivated to do this because when a network

device initially connects to a network the device seeks an address server from which to request a

network address, when done by the network administrator, it is a time consuming task,

performing the task automatically saves time.

In reference of claim 17, regarding computer-readable medium wherein the instructions for carrying out the steps of receiving a binding of a network address to an authenticated user of a client for which the policy enforcement point controls access to the network comprise instructions for carrying out the steps of performing network address binding resolution for the user.

Reid does not disclose steps for performing network address binding resolution for the user.

Ray discloses a method for allocation of a network address associated with a virtual subnet. The address server disclosed by Ray sends the network device an assigned network address, assigned by the address server and therefore assigned from an external binding process (column4 line 65 to column 5 line 31).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to automatically add nodes to the group as disclosed by Ray in the system of Reid. One of ordinary skill in the art would have been motivated to do this because when a network device initially connects to a network the device seeks an address server from which to request a network address, when done by the network administrator, it is a time consuming task, performing the task automatically saves time.

Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Reid in view of Ray and further in view of Cheng as applied to claim 1 above, and further in view of the article by Stewart.

Regarding the steps of receiving a binding of a network address to an authenticated user of a client for which the policy enforcement point controls access to the network comprises the steps of receiving an Internet Protocol (IP) address for the user from an ASAP protocol process.

Ray does not disclose a system receiving an Internet Protocol (IP) address for the user from an ASAP protocol process.

Stewart teaches the use of ASAP protocol for delivering messages (section 1.3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to ASAP as taught by Stewart in the system disclosed by Ray. One of ordinary skill in the art would have been motivated to do this because ASAP provides s high availability data transfer mechanism over IP network.

Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Reid in view of Ray and further in view of Cheng as applied to claim 1 above, and further in view of the Stevens.

Regarding the steps of receiving a binding of a network address to an authenticated user of a client for which the policy enforcement point controls access to the network comprises the steps of receiving an Internet Protocol (IP) address for the user from a DNS process.

Ray does not disclose a system for allocation of network address from a DNS process.

Stevens teaches the use of the DNS process to provide a protocol to allow clients and servers to communicate with each other by mapping hostnames and IP addresses.

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to use DNS as taught by Stevens in the name server disclosed by Ray. One of

ordinary skill in the art would have been motivated to do this because DNS is a well known

method of providing routing information; therefore other systems would be compatible with this

system.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).
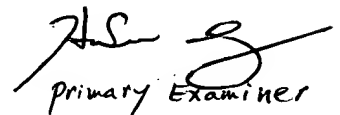
A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this

final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854.

The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Primary Examiner
AU 2135

PWK
Monday, June 13, 2005